# AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Jonathan Poole, Special Agent (SA) with the Drug Enforcement Administration (DEA) being duly sworn, depose and state as follows:

## I. PURPOSE OF THIS AFFIDAVIT

1. I submit this affidavit in support of a warrant authorizing the search of a silver LG cell phone bearing IMEI 356322-17-113519-5 **(the SUBJECT TELEPHONE).**

## II. AFFIANT BACKGROUND AND EXPERTISE

2. I am "an investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

3. I have been a Special Agent of the Drug Enforcement Administration ("DEA") since September 2017. I am currently assigned to the Baltimore District Office, Strike Force Group 1, which investigates drug trafficking organizations and their ties to violence. I received 19 weeks of training in narcotics investigations and related legal matters at the DEA Training Academy in Quantico, Virginia. Following graduation from the DEA Academy, I was assigned to the Atlanta Field Division Office and worked there until July of 2018, when I was assigned to the Baltimore District Office in Baltimore, MD. Prior to my employment as a Special Agent with the DEA, I was employed as a police officer/detective by the City of Suwanee Police Department for 4 years, two of which I spent assigned to the Gwinnett Metro Drug Task Force in Gwinnett County, Georgia.

4. During my time as a law enforcement officer, I have participated in numerous investigations involving drug trafficking to include the use of confidential informants, undercover

transactions, physical and electronic surveillance, telephone toll analysis, investigative interviews, the execution of search and seizure warrants, and the recovery of substantial quantities of narcotics, narcotics proceeds, and narcotics paraphernalia. I have reviewed recorded conversations, as well as documents and other records relating to narcotics trafficking and money laundering. I have examined records consisting in part of buyers and seller's lists, and pay/owe ledgers. I have interviewed drug dealers, drug users, and confidential informants and have discussed with them the lifestyles, appearances, and habits of drug dealers and drug users.

5. Through training, education and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed, the possession and use of firearms in connection with trafficking of such drugs, and the methods by which narcotics traffickers collect, store and conceal the proceeds of their illegal activities. I have also become familiar with the manner in which drug traffickers use telephones, cellular telephone technology, pagers, coded communications or slang-filled telephone conversations, false or fictitious identities, and other means to facilitate their illegal activities and thwart law enforcement investigations.

6. Through training, interviewing of dozens of persons arrested for controlled dangerous substance (CDS) offenses, watching hundreds of hours of surveillance of suspected drug traffickers, and monitoring of countless hours of intercepted communications involving drug trafficking, I am familiar with the actions, traits, habits, and terminology utilized by drug traffickers.

7. Based upon that training and experience, I have learned the following:

a. Drug traffickers keep and maintain records of their various activities. Such records are regularly concealed in a suspect's automobile, residence, office, and on his person, and that they take various forms. Documents commonly concealed by traffickers, include but are not limited to notes in code, deposit slips, wired money transactions, hidden bank accounts, photographs of co-conspirators, various forms of commercial paper, personal address books, notebooks, records, receipts, ledgers, travel receipts (rental receipts, airline tickets, bus tickets,

and/or train tickets) both commercial and private, money orders and other papers relating to the ordering, transportation, sale and distribution of controlled dangerous substances or other such documents which will contain identifying data on the co-conspirators. These items are kept in locations that are considered safe by the drug traffickers such as safety deposit boxes, residences, vehicles and on their person, where they have ready access to them. Drug traffickers often have several residences decreasing the likelihood of detection by law enforcement;

b. Drug traffickers may use computers or other electronic storage media, including smart phones, to store the records of documents listed in paragraph a;

c. Drug traffickers maintain on hand large amounts of cash to maintain and finance their narcotics business, which is typically concealed in their residences or vehicles along with financial instruments and evidence of financial transactions relating to narcotics trafficking activities;

d. Drug traffickers use cellular telephones, pagers and other electronic communications devices to facilitate illegal drug transactions. The electronically stored information on these devices is of evidentiary value in identifying other members of the drug trafficking conspiracy and establishing the relationship between these individuals, including photographs and other identifying information stored on these devices;

e. Drug traffickers commonly possess firearms and other weapons to protect and secure their narcotics and money from loss to law enforcement agents or other members of the criminal element that are motivated by greed; and

f. Drug traffickers commonly possess packaging material, cutting agents, digital scales, and other items used in the preparation and packaging of controlled substances.

8. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search the **SUBJECT TELEPHONE,** I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause. The information contained in this affidavit is based upon my personal knowledge, my review of documents and intercepted conversations, as well as conversations with other law enforcement officers and other individuals. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

## III. PROBABLE CAUSE

**A. BACKGROUND**

9. Since July of 2019, the Drug Enforcement Administration (DEA) has been investigating multiple violent drug trafficking organizations (DTOs) operating in the western section of Baltimore City. Based on evidence gathered to date, agents determined that the DTOs operate street-level shops and are believed to commit acts of violence associated with their drug trafficking activity. One of the shops being investigated is the "Master P" DTO. Albert SHIELDS has been identified as the street lieutenant of the DTO, and Torico REAVES has been identified as the leader and source of supply for the DTO. Michael BOWLES has been identified as the member of the DTO responsible for running the DTO's stash house. As part of the investigation, investigators have conducted controlled purchases and undercover purchases of fentanyl from a couple of DTO members, including Ti-Shika RUFFIN, Robert ROSS and Albert SHIELDS.

10. On November 12, 2019, the Honorable George L. Russell III, United States District Judge for the District Court of Maryland, authorized the interception of wire communications occurring over 443-943-2868 ("Target Telephone 1" or "TT1"), utilized by Albert SHIELDS. On November 26, 2019, Judge Russell authorized the continued interception of wire communications and the interception of electronic communications occurring over TT1. On December 12, 2019 and January 10, 2020, Judge Russell authorized the continued interception of both wire and electronic communications occurring over TT1. Also on January 10, 2020, Judge Russell authorized the interception of wire communications occurring over 202-766-8323 ("Target Telephone 2" or "TT2"), utilized by BOWLES. On February 7, 2020, Judge Russell again authorized the continued interception of wire communications over TT2.

**B. THE SUBJECT TELEPHONE**

11. As noted above, investigators identified SHIELDS and BOWLES as members of the Master P DTO during this investigation. SHIELDS was a street lieutenant for the DTO,

ensuring that street hitters had a supply of CDS for daily sales as well as conducting hand to hand transactions himself, usually with customers purchasing larger quantities. On a nearly daily basis, SHIELDS would use TT1 to communicate with BOWLES on TT2. These communications involved SHIELDS needing a resupply of CDS from BOWLES. SHIELDS would often obtain these resupplies from BOWLES multiple times in a day.

12. One such example of a resupply occurred on February 3, 2020. Investigators intercepted a call from BOWLES to SHIELDS at approximately 1:39 p.m. During this call, BOWLES asked SHIELDS, "What do you need?" SHIELDS replied, "Uh, five of them. I'll meet you in the split." BOWLES said, "I got you, alright." SHIELDS, near the end of the call, said, "I'm a call you when I get down there." At approximately 1:45 p.m., investigators intercepted a call from SHIELDS to BOWLES. During this call, SHIELDS said, "Everything look clear." BOWLES replied, "Here I come." Following this call, investigators saw BOWLES leave his stash house, 2436 Francis Street, Baltimore, MD and walk to a nearby break in the row homes, known to investigators as "the split," and referred to in the aforementioned intercepted call. Investigators, using a covert surveillance camera, saw BOWLES and SHIELDS meet briefly in the split before parting ways.

13. Based on my training and experience, I believe that BOWLES asked SHIELDS how much CDS he needed, with SHIELDS replying that he needed "five of them" and would meet BOWELS in "the split" (BOWLES asked SHIELDS, "What do you need?" SHIELDS replied, "Uh, five of them. I'll meet you in the split."). Additionally, I believe that SHIELDS told BOWLES that there were no law enforcement officers around, so the two could meet ("Everything look clear." BOWLES replied, "Here I come.") I further believe that the brief meeting investigators

observed in "the split" was the consummation of these meeting plans and the resupply of CDS that had been arranged using the Target Telephones.

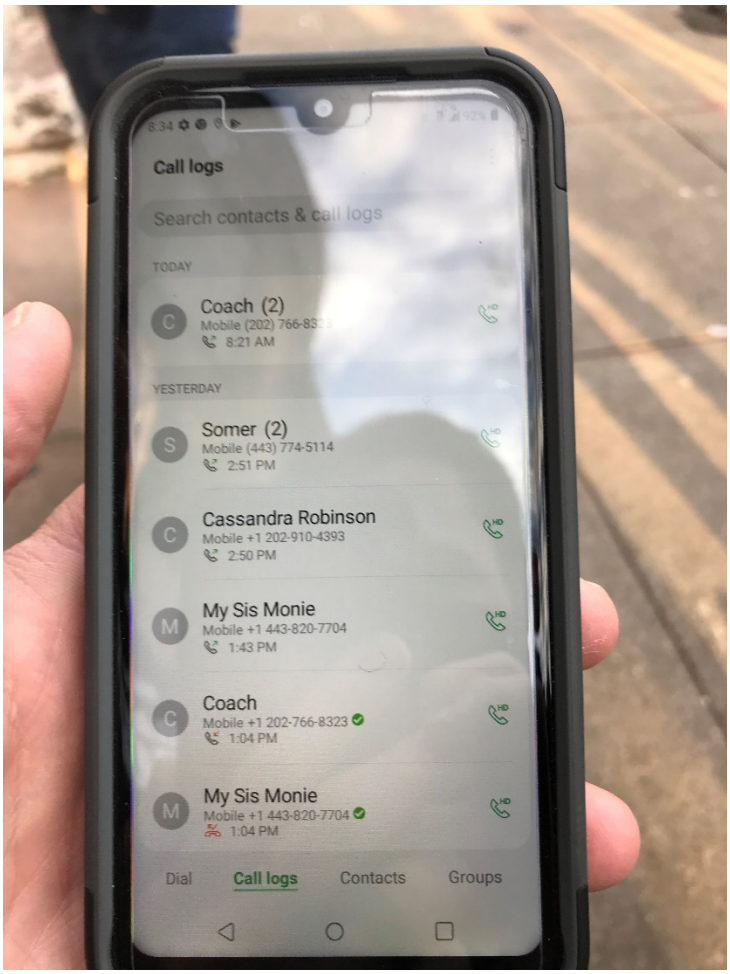
14. On April 5, 2020, the Honorable A. David Copperthite, U.S. Magistrate Judge for the District of Maryland, authorized search warrants for several locations associated with the Master P DTO. One of those locations was BOWLES's stash house, 2436 Francis Street, Baltimore, MD. This warrant was executed on April 14, 2020. BOWLES was located in the house during the execution of the warrant and approximately 196 grams of fentanyl (packaged in 850 gel caps for street sale) were seized along with CDS cutting agents.

15. On December 9, 2020, a grand jury in the District of Maryland returned an indictment charging a number of individuals associated with the Master P DTO, including SHIELDS and BOWLES, with drug trafficking offenses in violation of Title 18, United States Code, Sections 841 and 846.

16. On December 28, 2020, investigators located and arrested SHIELDS and BOWLES. SHIELDS was located sitting on a stoop in the area of DTO operations, the 2400 block of Woodbrook Avenue. BOWLES was located in his stash house, 2436 Francis Street. A search incident to SHIELDS's arrest revealed a pill bottle containing gel caps filled with a white powdery substance[1] and the **SUBJECT TELEPHONE**. SHIELDS was also in possession of a small amount of cash and a set of keys. Investigators asked SHIELDS who could take possession of the money and keys for him, as he would not be allowed to keep them with him in custody. SHIELDS asked investigators to call his sister, directing them to his cellular call log in the **SUBJECT TELEPHONE** in order to obtain his sister's number. While locating his sister's phone number in

[1] These gel caps appeared to be the same as the many purchased and seized during the investigation. The previous gel caps were determined to contain fentanyl following laboratory testing. The current gel caps were sent to the lab for testing with results pending.

the call log per SHIELDS's request, investigators saw two call records for a contact named "Coach[2]." The phone number assigned to this contact is 202-766-8323, previously identified as TT2. These two call log entries could be viewed on the screen at the same time SHIELDS's sister's number was displaying in the middle of the phone screen, and did not require investigators to scroll through the log to locate.




17. Based on the foregoing, I believe that there will be evidence of DTO operations located on the **SUBJECT TELEPHONE**, particularly communication between SHIELDS and

[2] Investigators know from previously intercepted communications that BOWLES's nickname is "Coach."

BOWLES, but also additional evidence between SHIELDS and other members of the DTO, identified and not yet identified.

## IV. BACKGROUND CONCERNING ELECTRONIC COMMUNICATIONS DEVICES

18. I am familiar with the mode of operation of individuals who commit drug trafficking offenses, including, but not limited to, their use of electronic devices to plan and coordinate drug trafficking activities. Based on my knowledge, training, and experience, individuals committing drug trafficking offenses frequently use cellular telephones, communication devices, and other electronic media storage to further their illegal activities. Based upon my training, experience and participation in this and other investigations, I know the following:

19. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity. All of the above cell phones have both digital storage capacity and digital camera capabilities.

20. Individuals engaged in drug trafficking offenses often use cell phones to communicate with suppliers, to place orders with suppliers, to communicate with customers, to receive orders from customers, and to arrange meeting times and locations for the distribution of controlled substances. The individuals engaging in drug trafficking will often use a combination of voice calls and text messages to coordinate drug transactions. Individuals engaged in drug trafficking offenses also use digital storage devices to maintain telephone number "contact lists" of individuals who may have assisted in the planning of this and other criminal activity.

21. Drug trafficking is an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, drug trafficking is an illegal commercial activity that is characterized by regular, repeated criminal activity.

22. Cellular telephones are an indispensable tool of the narcotics trafficking trade. Narcotic traffickers use cellular telephones, push-to-talk telephones, Short Message Service ("SMS"), electronic-mail, and similar electronic means and/or devices, often under fictitious names or names other than their own, in order to maintain contact with other conspirators and narcotic traffickers. In addition, narcotic traffickers will often change their cellphones following the arrest of a member of their Drug Trafficking Organization ("DTO"), or at random in order to frustrate law enforcement efforts.

23. Narcotic traffickers often place nominal control and ownership of telephones in names other that their own to avoid detection of those telephones by government agencies. Even though telephones are in the names of other people, drug traffickers retain actual ownership, control, and use of the telephone, exercising dominion and control over them.

24. Drug traffickers utilize different types of communication devices, and change the numbers to these communication devices frequently. This is done to avoid detection by law enforcement personnel. I also know that drug traffickers will dedicate different communication devices for different aspects of the trafficking organization. An example of this would be a drug trafficker utilizing one cellular telephone to communicate with customers, and utilizing another cellular telephone to communicate with a source of supply of drugs.

25. Cellular phones associated with drug traffickers include various types of evidence. Phones may contain relevant text messages or other electronic communications; they may contain electronic address books listing the phone numbers and other contact information associated with co-conspirators; and they may contain other types of information.

26. The mere fact of a cellular phone's call number, electronic serial number or other identifying information may be evidentiary value as it may confirm that a particular cell phone is the phone identified during a wiretap, pen register, or other electronic investigation.

## V. FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

27. Based on my knowledge, training, and experience, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT TELEPHONE** may still be stored on those devices, for various reasons, as discussed in the following paragraphs.

28. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT TELEPHONE** was used, the purpose of its use, who used it, and when.

29. There is probable cause to believe that this forensic electronic evidence might be on the Device because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the

times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

30. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

31. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

32. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

33. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

35. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

36. During this case and in numerous others involving complex DTOs, investigators have learned that the drug-trafficking organization relies heavily on electronic devices to facilitate drug trafficking. It is necessary to conduct a physical inspection of the electronic devices in order to obtain electronic communications and other information that might be stored on the seized phones and to determine whether any of the seized phones were the subject of wiretap, pen register or other investigation detailed herein. The phones may also contain data and communications that were not electronically intercepted due to encryption or for other reasons.

37. Again, the **SUBJECT TELEPHONE** remains in the custody of law enforcement. The only known specifics of each phone requested for authorization to search are detailed in Attachment A and the types of information expected to be recovered from the devices are listed in Attachment B.

## VI. CONCLUSION

38. Accordingly, there is probable cause to believe that evidence will be found from an analysis of the **SUBJECT TELEPHONE** recovered. The **SUBJECT TELEPHONE** may contain the records of SHIELDS' calls, which may include calls with BOWLES and other persons involved in the Master P DTO operations. The phone may contain copies of SMS or text or other electronic communications relating to activities associated with the DTO. The phones may also contain a variety of other electronic evidence, including electronic communications through various cellular or internet-based applications, photographs and other information.

39. Wherefore, in consideration of the facts presented, I respectfully request that this Court issue search warrants for the **SUBJECT TELEPHONE,** and authorize the search and seizure of the items described in Attachment A, for the information set forth in Attachment B, where applicable, which constitute fruits, evidence and instrumentalities of conspiracy to distribute and possess with intent to distribute controlled substances, in violation of 21 U.S.C. § 846, and possession with intent to distribute controlled substances, in violation of 21 U.S.C. § 841.

## VII. REQUEST FOR NIGHT-TIME AUTHORIZATION

40. There is good cause for the Court to authorize the requested searches at any time of the day or night. The **SUBJECT TELEPHONE** are already in law enforcement custody, and it is reasonable to allow law enforcement to execute the requested searches at any hour of the day, even during the evening or night, if doing so is convenient for the investigators or examiners. Because the devices are in law enforcement custody already, there will be prejudice to any other person from this request.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Special Agent Jonathan Poole
Drug Enforcement Administration

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 22 day of January, 2021.

Thomas M. DiGirolamo
United States Magistrate Judge

**ATTACHMENT A**
**Device to be Searched**

This warrant applies to information associated with a silver LG cell phone bearing IMEI 356322-17-113519-5 (the "**SUBJECT TELEPHONE**"), which is currently in the custody of the Drug Enforcement Administration at a secure facility located in Baltimore, Maryland.

**ATTACHMENT B**
**ITEMS TO BE SEIZED**

All records contained in the item described in Attachment A (the "Subject Telephone" or "Device") which constitute evidence of violations of 21 U.S.C. §§ 846 and 841(a)(1), including but not limited to the following:

1. All of the following records, in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form, including but not limited to:

    a. Contact logs that refer or relate to the user of any and all numbers on the Subject Telephone;

    b. Call logs reflecting date and time of received calls;

    c. Any and all digital images and videos of persons associated with this investigation;

    d. Text messages to and from the Subject Telephone that refer or relate to the crimes under investigation;

    e. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation;

    f. Voicemails that refer or relate to the crimes under investigation;

    g. Voice recordings that refer or relate to the crimes under investigation;

    h. Any data reflecting the phone's location;

    i. Contact lists;

    j. Data from third-party applications (including social media applications like Facebook and Instagram and messaging programs like WhatsApp and Snapchat);

    k. Browser history; and

    l. Bank records, checks, credit card bills, account information, and other financial records.

2. Any and all records related to the location of the user(s) of the devices.

3. For the Device:

    a. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Device;

f. evidence of the times the Device was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the Device;

h. documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device;

i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

6. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.